

Requested Patent: JP2001013870A

Title:

METHOD OF COMMON KEY ENCIPHERING OR DECIPHERING, AND RECORDING  
MEDIUM WITH COMMON KEY CIPHERING OR DECIPHERING PROGRAM  
RECORDED THEREON ;

Abstracted Patent: JP2001013870 ;

Publication Date: 2001-01-19 ;

Inventor(s): IMOTO AKIO ;

Applicant(s): NEC CORP ;

Application Number: JP19990184453 19990629 ;

Priority Number(s): ;

IPC Classification: G09C1/00; H04L9/06 ;

Equivalents: ;

#### ABSTRACT:

PROBLEM TO BE SOLVED: To provide a common key ciphering method virtually disabling a known plaintext attack and a selected plaintext attack. SOLUTION: The disclosed common key enciphering method enciphers a plaintext by preparing a table of random digits and a reading mechanism 1, an indirect index array 2, and a four-dimensional matrix 4 with constant coefficients beforehand, deciding display start positions of each step of the table of random digits from a secret key 6, calculating (p+q) pieces of original maps by the table of random digits and the reading mechanism 1 every time m-bytes of character string is taken out of a plaintext, generating a 1st indirect index array presenting a composited map of the p-pieces of original map numbers and a 2nd indirect index array presenting a composited map of the q-pieces of original map numbers, converting the character string taken out of the plaintext data by the 1st indirect index array, converting the character string of this conversion result by integrating it with m-dimensional matrix with constant coefficients, and storing in the ciphertext a character string obtained by converting the character string of the conversion result by the 2nd indirect index array.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-13870  
(P2001-13870A)

(43) 公開日 平成13年1月19日 (2001.1.19)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 Z 5 J 1 0 4
H 0 4 L 9/06		H 0 4 L 9/00	6 1 1 Z

審査請求 有 請求項の数 8 O L (全 16 頁)

(21) 出願番号 特願平11-184453

(22) 出願日 平成11年6月29日 (1999.6.29)

(71) 出願人 000004237

日本電気株式会社  
東京都港区芝五丁目7番1号

(72) 発明者 井本 明夫

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100099830

弁理士 西村 征生

Fターム(参考) 5J104 A4D1 JA13 JA15 NA10

(54) 【発明の名称】 共通鍵暗号化又は復号化方法と、共通鍵暗号化又は復号化プログラムを記録した記憶媒体

(57) 【要約】

【課題】 既知平文攻撃並びに選択平文攻撃を事実上不可能とする、共通鍵暗号化方法を提供する。

【解決手段】 開示される共通鍵暗号化方法は、乱数表と読み出し機構1と、間接指標配列2と、定数係数の4次行列4を予め用意し、秘密鍵6から乱数表の各段の表示開始位置を決定して、平文データからmバイトの文字列を取り出すごとに、乱数表と読み出し機構1によって、(p+q)個の原写像の番号を算出し、p個の原写像番号の合成写像を表す第1の間接指標配列と、q個の原写像番号の合成写像を表す第2の間接指標配列とを作成して、平文データから取り出された文字列を第1の間接指標配列で変換し、変換結果の文字列を定数係数のm次行列との積算で変換し、この変換結果の文字列を第2の間接指標配列で変換して得た文字列を、暗文データ中に格納することによって、平文の暗号化を行う。

対象文字が89種の場合の文字—数値間の対応の例

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
&	'	(	)	*	+	.	-	.	/	0	1	2	3	4	5
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
6	7	8	9	:	:	<	=	>	?	@	A	B	C	D	E
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
V	W	X	Y	Z	[	¥	]	^	_	`	a	b	c	d	e
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
80	81	82	83	84	85	86	87	88							
v	w	x	y	z	{		}	~							

## 【特許請求の範囲】

【請求項1】 長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数の $m$ 次行列とを予め用意し、

秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

平文データから $m$ バイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の合成写像を表す第2の間接指標配列とを作成して、前記平文データから取り出された文字列を前記第1の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果の文字列を前記第2の間接指標配列で変換して得た文字列を、暗文データ中の $m$ バイトの文字列として暗文データに格納する処理を、前記平文データからの $m$ バイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴とする共通鍵暗号化方法。

【請求項2】 長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

暗文データから $m$ バイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第2の間接指標配列とを作成して、前記暗文データから取り出された文字列を前記第2の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果の文字列を前記第1の間接指標配列で変換して得た文字列を、平文データ中の $m$ バイトの文字列として平文データに格納する処理を、前記暗文データからの $m$ バイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うことを特徴とする共通鍵復号化方法。

【請求項3】 長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係

数の $m$ 次行列とを予め用意し、

秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

平文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記 $(p+q)$ 個の原写像の番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を第2の作業ベクトルに格納し、前記平文データから取り出したベクトルの各要素を、前記第1の作業ベクトルの各要素に含まれる、前記 $p$ 個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を前記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第2の作業ベクトルの各要素に含まれる、前記 $q$ 個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中の $m$ バイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからの $m$ バイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴とする共通鍵暗号化方法。

【請求項4】 長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

暗文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記 $(p+q)$ 個の原写像番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を暗号化時と逆順に第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を暗号化時と逆順に第2の作業ベクトルに格納し、前記暗文データから取り出したベクトルの各要素を、前記第2の作業ベクトルの各要素に含まれる、前記 $q$ 個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクトルの各要素を前記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第1の作業ベクトルの各要素に含まれる、前記 $p$ 個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中の $m$ バイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからの $m$ バイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつず

らしながら繰り返すことによって、暗文の復号化を行うことを特徴とする共通鍵復号化方法。

【請求項5】 請求項1記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数の $m$ 次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データから $m$ バイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の合成写像を表す第2の間接指標配列とを作成して、前記平文データから取り出された文字列を前記第1の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果の文字列を前記第2の間接指標配列で変換して得た文字列を、暗文データ中の $m$ バイトの文字列として暗文データに格納する処理を、前記平文データからの $m$ バイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴とする共通鍵暗号化プログラムを記録した記憶媒体。

【請求項6】 請求項2記載の共通鍵復号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データから $m$ バイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第2の間接指標配列とを作成して、前記暗文データから取り出された文字列を前記第2の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果の文字列を前記第1の間接指標配列で変換して得た文字列を、平文データ中の $m$ バイトの文字列として平文データに格納する処理を、前記暗文データからの $m$ バイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復

号化を行うプログラムを記録したことを特徴とする共通鍵復号化プログラムを記録した記憶媒体。

【請求項7】 請求項3記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数の $m$ 次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記 $(p+q)$ 個の原写像の番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を第2の作業ベクトルに格納し、前記平文データから取り出したベクトルの各要素を、前記第1の作業ベクトルの各要素に含まれる、前記 $p$ 個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を前記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第2の作業ベクトルの各要素に含まれる、前記 $q$ 個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中の $m$ バイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからの $m$ バイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴とする共通鍵暗号化プログラムを記録した記憶媒体。

【請求項8】 請求項4記載の共通鍵復号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記 $(p+q)$ 個の原写像の番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を暗号化時と逆順に第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を暗号化時と逆順に第2の作業ベクトルに格納し、前記暗文データから取り出したベクトルの各要素を、前記第2の作業ベクトルの各要素に含まれる、前記 $q$ 個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクトル

ルの各要素を前記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第1の作業ベクトルの各要素に含まれる、前記 $p$ 個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中の $m$ バイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからの $m$ バイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うプログラムを記録したことを特徴とする共通鍵復号化プログラムを記録した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化処理と復号化処理とに共通の秘密鍵を用いる、共通鍵暗号化又は復号化方法並びに共通鍵暗号化又は復号化プログラムを記録した記憶媒体に関する。

【0002】

【従来の技術】従来、この種の暗号化方式は、秘密鍵の内容を知らずに、暗号文に対して解読を試みる攻撃者に対して、暗号化されたデータの安全性を確保することを目的として用いられている。例えば、ブロック型暗号化方式としては、現在、米国において標準化されている暗号化規格である、DES (Data Encryption Standard) 暗号によるものが、広く使用されている。しかしながら、DESでは、選択平文攻撃によって、差分解法と呼ばれる手段で解読され、また、既知平文攻撃によって、線形解読法と呼ばれる手段で解読される危険がある。これは、DESでは、転置以外には、排他的論理和という、線形の性質を持つ変換しか行っていないためである。

【0003】また、DESは、計算機上のプログラムとしては、処理が遅いが、これによって、攻撃者が専用のハードウェアを用いた場合に、攻撃者だけが有利になって、利用者が不利になるという欠点につながる。これは、DESは、転置及びビットごとの排他的論理和という、計算機上では実行速度の遅い処理を多用しているためである。これに対して、特開平10-123949号(特願平9-217299号)公報には、DES暗号を改良して、差分解法に対して安全性を強化する技術が開示されている。しかしながら、この従来技術によっても、依然として、計算機上のプログラムとしては、処理が遅いという問題が残っている。これは、この従来技術においても、やはり、ビット転置という、計算機上では実行速度の遅い処理が多用されているためである。

【0004】一方、別の暗号化方式として、ストリーム型暗号化方式がある。例えば、特開平9-288565号(特願平8-99985号)公報においては、カオス軌道に沿った実数値の乱数列を生成して使用する技術が開示されている。しかしながら、この従来技術では、ア

ーキテクチャの異なる複数の計算機上で、同じ動作を保証することが困難であるという問題がある。これは、実数値の乱数列を、実数演算の繰返しによって算出するので、計算機のアーキテクチャの僅かな違いによって、発生する乱数列が異なるものになってしまうことがあるためである。また、上記の従来技術では、乱数列が短周期に陥る危険性に関して、このような危険の回避を保証できないという問題がある。これは、カオスを発生する自励系の実数演算では、周期点を発見することが難しい反面、短周期に陥っていないことの保証もしていないためである。

【0005】

【発明が解決しようとする課題】この発明は、上述の事情に鑑みてなされたものであって、暗号化処理と復号化処理とに共通の鍵を用いる、共通鍵暗号化方式であって、既知平文攻撃並びに選択平文攻撃を、事実上不可能にする、共通鍵暗号化又は復号化方法並びに共通鍵暗号化又は復号化プログラムを記録した記憶媒体を提供することを目的としている。

【0006】

【課題を解決するための手段】上記課題を解決するため、請求項1記載の発明は、共通鍵暗号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個( $p, q$ は任意の自然数。以下、省略)の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数の $m$ 次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データから $m$ バイトの文字列を取り出すごとに、上記乱数表と読み出し機構によって、上記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の合成写像を表す第2の間接指標配列とを作成して、上記平文データから取り出された文字列を上記第1の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果の文字列を上記第2の間接指標配列で変換して得た文字列を、暗文データ中の $m$ バイトの文字列として暗文データに格納する処理を、上記平文データからの $m$ バイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴としている。

【0007】また、請求項2記載の発明は、共通鍵復号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データから $m$ バイトの文字列

を取り出すごとに、上記乱数表と読み出し機構によって、上記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第2の間接指標配列とを作成して、上記暗文データから取り出された文字列を上記第2の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果の文字列を上記第1の間接指標配列で変換して得た文字列を、平文データ中の $m$ バイトの文字列として平文データに格納する処理を、上記暗文データからの $m$ バイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うことを特徴としている。

【0008】また、請求項3記載の発明は、共通鍵暗号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数の $m$ 次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記 $(p+q)$ 個の原写像の番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を第2の作業ベクトルに格納し、上記平文データから取り出したベクトルの各要素を、上記第1の作業ベクトルの各要素に含まれる、上記第 $p$ 個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第2の作業ベクトルの各要素に含まれる、上記第 $q$ 個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中の $m$ バイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからの $m$ バイトの所定数の要素分のベクトルの読み出しごとに、上記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴としている。

【0009】また、請求項4記載の発明は、共通鍵復号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始

位置を決定したのち、暗文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記 $(p+q)$ 個の原写像の番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を暗号化時と逆順に第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を暗号化時と逆順に第2の作業ベクトルに格納し、上記暗文データから取り出したベクトルの各要素を、上記第2の作業ベクトルの各要素に含まれる、上記 $q$ 個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第1の作業ベクトルの各要素に含まれる、上記 $p$ 個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中の $m$ バイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからの $m$ バイトの所定数の要素分のベクトルの読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うことを特徴としている。

【0010】また、請求項5記載の発明は、共通鍵暗号化プログラムを記録した記憶媒体に係り、請求項1記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数の $m$ 次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データから $m$ バイトの文字列を取り出すごとに、上記乱数表と読み出し機構によって、上記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の合成写像を表す第2の間接指標配列とを作成して、上記平文データから取り出された文字列を上記第1の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果の文字列を上記第2の間接指標配列で変換して得た文字列を、暗文データ中の $m$ バイトの文字列として暗文データに格納する処理を、上記平文データからの $m$ バイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴としている。

【0011】また、請求項6記載の発明は、共通鍵復号化プログラムを記録した記憶媒体に係り、請求項2記載の共通鍵復号化方法を実行するプログラムを記録したコ

ンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データから $m$ バイトの文字列を取り出すごとに、上記乱数表と読み出し機構によって、上記 $(p+q)$ 個の原写像の番号の算出を行い、該 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第1の間接指標配列と、前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第2の間接指標配列とを作成して、上記暗文データから取り出された文字列を上記第2の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果の文字列を上記第1の間接指標配列で変換して得た文字列を、平文データ中の $m$ バイトの文字列として平文データに格納する処理を、上記暗文データからの $m$ バイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うプログラムを記録したことを特徴としている。

【0012】また、請求項7記載の発明は、共通鍵暗号化プログラムを記録した記憶媒体に係り、請求項3記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数の $m$ 次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記 $(p+q)$ 個の原写像の番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を第2の作業ベクトルに格納し、上記平文データから取り出したベクトルの各要素を、上記第1の作業ベクトルの各要素に含まれる、上記 $p$ 個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数の $m$ 次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第2の作業ベクトルの各要素に含まれる、上記 $q$ 個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中の $m$ バイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからの $m$ バイトの所定数の要素分のベク

トルの読み出しごとに、上記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴としている。

【0013】また、請求項8記載の発明は、共通鍵復号化プログラムを記録した記憶媒体に係り、請求項4記載の共通鍵復号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき $(p+q)$ 個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数の $m$ 次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データから $m$ バイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記 $(p+q)$ 個の原写像の番号の算出を行って、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $p$ 個の原写像番号を暗号化時と逆順に第1の作業ベクトルに格納するとともに、要素ごとに使用する前記 $(p+q)$ 個の原写像番号中の $q$ 個の原写像番号を暗号化時と逆順に第2の作業ベクトルに格納し、上記暗文データから取り出したベクトルの各要素を、上記第2の作業ベクトルの各要素に含まれる、上記 $q$ 個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数の $m$ 次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第1の作業ベクトルの各要素に含まれる、上記 $p$ 個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中の $m$ バイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからの $m$ バイトの所定数の要素分のベクトルの読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うプログラムを記録したことを特徴としている。

【0014】

【作用】この発明の構成では、平文の暗号化を行う場合には、秘密鍵が与えられると、乱数表と読み出し機構の上での表示開始位置が定まる。次に、平文データから、平文データ中の $m$ バイト文字列を読み出す度に、乱数表と読み出し機構から値を読み出して、使用する $(p+q)$ 個の原写像の番号を決定する。平文データ中の $m$ バイトの文字列は、まず原写像の $p$ 個の原写像番号の合成写像である間接指標配列によって変換され、次に $m$ 次の行列との積算によって変換され、最後に、原写像の $q$ 個の原写像番号の合成写像である間接指標配列によって変換されて、暗文データ中の $m$ バイトの文字列が生成される。逆に、暗文の復号化を行う場合には、秘密鍵が与えられると、乱数表と読み出し機構の上での表示開始位置が定まる。次に、暗文データから、暗文データ中の $m$ バ

イト文字列を読み出す度に、乱数表と読み出し機構から値を読み出して、使用する $(p+q)$ 個の原写像の番号を決定する。暗文データ中の $m$ バイト文字列は、まず原写像の $q$ 個の原写像番号の逆順の逆写像の合成写像である間接指標配列によって変換され、次に $m$ 次の行列の逆行列との積算によって変換され、最後に、原写像の $p$ 個の原写像番号の逆順の逆写像の合成写像である間接指標配列によって変換されて、平文データ中の $m$ バイトの文字列が生成される。

【0015】また、この発明の別の構成では、平文の暗号化を行う場合には、秘密鍵が与えられると、乱数表の上での表示開始位置が定まる。次に、平文データから、平文データ中の $m$ バイト×所定要素数のベクトルを読み出す度に、乱数表と読み出し機構から値を読み出して、使用する $(p+q)$ 個の原写像の番号を決定する。平文データ中の $m$ バイト×所定要素数のベクトルは、まず要素ごとに使用する $p$ 個の原写像番号を格納した作業ベクトルの原写像を用いて変換（リストベクトルロード）され、次に $m$ 次の行列との積算によって変換され、最後に、要素ごとに使用する $q$ 個の原写像番号を格納した作業ベクトルの原写像を用いて変換（リストベクトルロード）されて、暗文データ中の $m$ バイト×所定要素数のベクトルが生成される。逆に、暗文の復号化を行う場合には、秘密鍵が与えられると、乱数表の上での表示開始位置が定まる。次に、暗文データから、暗文データ中の $m$ バイト×所定要素数のベクトルを読み出す度に、乱数表と読み出し機構から値を読み出して、使用する $(p+q)$ 個の原写像の番号を決定する。暗文データ中の $m$ バイト×所定要素数のベクトルは、まず要素ごとに使用する $q$ 個の原写像番号を、逆順に格納した作業ベクトルの逆写像を用いて変換（リストベクトルロード）され、次に、 $m$ 次の逆行列との積算によって変換され、最後に、要素ごとに使用する $p$ 個の原写像番号を、逆順に格納した作業ベクトルの逆写像を用いて変換（リストベクトルロード）されて、平文データ中の $m$ バイト×所定要素数のベクトルが生成される。

$$Z \mid 89 = \{0, 1, \dots, 88\}$$

なお、剰余類の法、すなわち対象とする文字の種類の数  
が素数でない場合には、後述する定数係数行列の選択において、特別の注意が必要である。

【0020】次に、この発明において用いられる間接指標配列による写像の仕組みについて説明する。図2は、この発明の実施の形態における間接指標配列による写像の仕組みについて示したものであって、(a)は指標と間接指標配列による写像の説明、(b)は写像の例、(c)は合成写像の例をそれぞれ示している。図2(a)に示すように、指標 $x$ を間接指標配列 $c(j)$  ( $j=0\sim 88$ )で変換すると、 $y=c(x)$ になる。指標配列 $x(i)$  ( $i=0\sim 3$ )を、間接指標配列 $c(j)$  ( $j=0\sim 88$ )で変換すると、配列 $y(i)=$

【0016】したがって、この発明による暗文に対して、秘密鍵を知らずに解読を試みる者にとっては、既知平文攻撃から乱数表と読み出し機構の上での表示開始位置を知ることができない。また、既知の平文と暗文の組み合わせ、又は選択した平文と暗文の組み合わせから、差分をとって解析することもできない。また、選択平文攻撃を繰り返して、平文 $m$ バイトの総当たりを試行することも事実上できない。また、秘密鍵を総当たりで試行することもできない。また、間接指標配列を総当たりで試行することも、間接指標配列の原写像の順列の総当たりを試行することもできない。このように、この発明によれば、データを暗号化する場合に、長周期の乱数表と、乱数によって間接指標配列の順列を変化させる機構と、間接指標配列による変換で定数系列行列との積算を挟む形の合成写像とを用いることによって、既知平文攻撃並びに選択平文攻撃を、事実上不可能にすることができる。

【0017】

【発明の実施の形態】最初に、この発明の実施の形態において用いられる写像の仕組みについて、図を参照しながら、簡単に説明する。

【0018】近代以降の暗号においては、対象とする範囲の文字を、何らかの手法で数値と対応させることが必須である。対象とする文字の範囲は、前提とする通信路の種類によってさまざまである。また、文字と数値との対応のさせかたも、使用する暗号化の方式によっていろいろである。

【0019】図1は、写像において、文字と数値を対応させる場合の例を示し、対象文字が89種類の場合の、文字-数値間の対応を例示している。図1に示された例では、英字、数字、及びいくつかの記号を含む89種類の文字を対象とした場合に、 $0\sim 88$ の整数値と対応させた例を示している。以降の説明においては、89種類の文字を、89を法とする剰余類の元と同一視するものとし、89を法とする剰余類を $Z \mid 89$ と表記する（式(1)参照）。

$$\dots (1)$$

$c(x(i))$ になる。図2(b)に示すように、指標配列 $(50, 60, 70, 80)$ を、間接指標配列 $(2(0番), 3, \dots, 52(50番), \dots, 62(60番), \dots, 88(86番), 0, 1(88番))$ で変換すると、配列 $(52, 62, 72, 82)$ になる。また、図2(c)に示すように、指標配列 $(50, 60, 70, 80)$ を、間接指標配列 $(2(0番), 3, \dots, 52(50番), \dots, 62(60番), \dots, 88(86番), 0, 1(88番))$ で変換し、さらに、間接指標配列 $(1(0番), 2, 3, \dots, 53(52番), \dots, 63(62番), \dots, 83(82番), \dots, 88, 0(88番))$ で変換すると、配列 $(53, 63, 73, 83)$ になる。



【0021】この発明の実施の形態における以降の説明において、間接指標配列とは、 $Z \mid 89$ の元を1個ずつ任意の順序で配列したものである。すなわち、 $c(j)$

$$\forall j \in Z \mid 89$$

$$c(j) \in Z \mid 89$$

$$\forall i, j \in Z \mid 89$$

$$i \neq j \rightarrow c(i) \neq c(j)$$

間接指標配列は、1個の元又は任意の個数の元の配列を、別の文字で置き換える旨の、全単射の写像を表すことができる。変換される対象となる文字を $x$ とすると、当然、 $x \in Z \mid 89$ である。これを間接指標配列 $c$

( $j$ )で変換した写像の行き先は、 $c(x)$ である。間接指標配列は、何個かの元の配列を変換することもできる。例えば、変換される対象となる4個の文字の配列を、 $x(i)$  ( $i=0 \sim 3$ )とすると、当然、 $0 \leq i \leq 3$ のそれぞれの $i$ について、 $x(i) \in Z \mid 89$ である。これを間接指標配列 $c(j)$ で変換した写像の行き先は、 $c(x(i))$ である。

【0022】以降の説明では、変換される対象となる元又は元の配列を、指標又は指標配列と呼ぶ。これは、変換される対象の元が、間接指標配列の添字として、行き先を示す指標となっているためである。間接指標配列による写像の合成写像は、間接指標配列で表すことができる。間接指標配列 $c1(j)$ 、 $c2(j)$  ( $i=0 \sim 88$ )があったとき、指標 $x$ をまず $c1(j)$ で変換し、それから $c2(j)$ で変換した合成写像の行き先は、 $c2(c1(x))$ である。 $c1(j)$ による変換に続いて $c2(j)$ による変換を行うという合成写像は、間接指標配列 $c2(c1(j))$ で表される。

【0023】図3は、この発明の実施の形態における間接指標配列による写像の逆写像について示したものであって、(a)は逆写像を表す間接指標配列の説明、(b)は逆写像を表す間接指標配列の例をそれぞれ示している。

【0024】図3(a)に示すように、指標配列 $x(i)$  ( $i=0 \sim 88$ )を間接指標配列 $c(j)$  ( $j=0 \sim 88$ )で変換して、配列 $(0, 1, \dots, 88)$ になる場合、配列 $x(i)$  ( $i=0 \sim 88$ )を間接指標配列とみなして表される写像は、配列 $c(j)$ の表す写像の逆写像である。

【0025】図3(b)に示すように、指標配列 $(87, 88, 0(2番), 1, \dots, 48(50番), \dots, 58(60番), \dots, 85(87番), 86(88番))$ を、間接指標配列 $(2(0番), 3, \dots, 52(50番), \dots, 62(60番), \dots, 88(86番), 0, 1(88番))$ で変換すると、配列 $(0, 1, 2, \dots, 87, 88)$ になる。

【0026】間接指標配列による写像には、必ず1個の逆写像が存在する。任意の間接指標配列 $c(j)$  ( $j=0 \sim 88$ )に対して、ただ1個の指標配列 $x(j)$  ( $j=0 \sim 88$ )が間接指標配列である場合は、式

(2)及び式(3)に示す関係が成り立つ。

$$\dots(2)$$

$$\dots(3)$$

$=0 \sim 88$ )が存在し、 $c(x(j)) = (0, 1, \dots, 88)$ となる。なぜならば、定義から、間接指標配列とは、 $Z \mid 89$ の元が1個ずつ並んだものだからである。 $(0, 1, \dots, 88)$ は、恒等写像であるから、上記の場合に、 $x(j)$ は $c(j)$ による変換の逆写像を表す間接指標配列である。

【0027】図4は、この発明の実施の形態における行列の積算による写像の仕組みについて示したものであって、(a)は行列の積算による写像の説明、(b)は行列の積算による写像の例をそれぞれ示している。図4(a)に示すように、指標配列 $x(i)$  ( $i=0 \sim 3$ )を、行列 $f(i, j)$  ( $i, j=0 \sim 3$ )との積算で変換すると、式(4)に示す配列が与えられる。

【0028】

【数1】

$$y(i) = \sum_{j=0}^3 (f(i, j) * x(j)) \quad \dots(4)$$

【0029】図4(b)に示すように、配列 $(1, 2, 3, 4)$ を、式(5)に示す行列との積で変換すると、式(6)で表される指標配列 $(1, 3, 4, 5)$ になる。

【0030】

【数2】

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad \dots(5)$$

【0031】

【数3】

$$\begin{pmatrix} 1 \\ 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \quad \dots(6)$$

【0032】行列の積算による写像の仕組みは、次のようなものである。いま、 $x(i)$ は $Z \mid 89$ の元を、いくつか並べた配列であって、例えば、4個の要素を持つ配列とする。4次の正方行列 $f(i, j)$  ( $i, j=0 \sim 3$ )があったとき、89を法とする行列とベクトルとの積 $f \cdot x$ は、 $Z \mid 89$ の元を4個並べた配列である。 $n$ 次の正方行列の積算は、 $Z \mid 89$ の元を4個並べた配列から、 $Z \mid 89$ の元を4個並べた配列への写像である。

【0033】図5は、この発明の実施の形態における逆行列の積算による逆写像の仕組みについて示したもので

あって、(a)は逆行列の積算による逆写像の説明、  
(b)は逆写像を表す逆行列の例をそれぞれ示している。図5(a)に示すように、行列 $g(i, j)$  ( $i, j=0\sim3$ )と、行列 $f(i, j)$  ( $i, j=0\sim3$ )との積が単位行列である場合、行列 $g$ との積算による変

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 88 & 1 & 0 & 0 \\ 88 & 0 & 1 & 0 \\ 88 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 89 & 1 & 0 & 0 \\ 89 & 0 & 1 & 0 \\ 89 & 0 & 0 & 1 \end{pmatrix} \\ \stackrel{(\text{mod } 89)}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \dots (7)$$

【0035】行列 $g$ との積算による変換は、行列 $f$ との積算による変換の逆写像である。逆行列の積算による逆写像の仕組みは、次のようなものである。いま、行列 $f$ に対して、逆行列 $g$ が存在したとき、行列 $g$ の積算による写像は、行列 $g$ の積算による写像の逆写像を表す。

【0036】逆行列は、任意の行列 $f$ に対して常に存在するわけではない。特に、剰余類の法として素数でない数を選んだときは、注意が必要である。この発明の実施例では、定数係数の行列 $f$ と定数係数の逆行列 $g$ との組み合わせを用いる。行列 $f$ に対して、逆行列が存在する場合、行列 $f$ は、 $Z \mid 89$ の元を4個並べた配列から、 $Z \mid 89$ の元を4個並べた配列への、全単射の写像である。

【0037】以下、図面を参照して、この発明の実施の形態について説明する。説明は、実施例を用いて具体的にを行う。

#### ◇第1実施例

図6は、この発明の第1実施例である共通鍵暗号化又は復号化方法において、使用開始以前に決定し配布される事項を説明する図、図7、図8は、同実施例の方法における暗号化と復号化の手順を説明する図である。この例においては、図6に示す、乱数表と読み出し機構1と、原写像0～67を表す間接指標配列2と、原写像0～67の逆写像を表す間接指標配列3と、定数係数の4次行列 $f$ 4と、 $f$ の逆行列 $g$ 5とは、共通鍵暗号化又は復号化方法の使用開始以前に、別途決定され、配布されているものとする。

【0038】乱数表と読み出し機構1は、ランダムな整数値を収容した10段の乱数表を装備している。この乱数表の各段の長さは、順に、89, 83, 79, ..., 47のように、互いに素の関係になっている。読み出し機構は、適当な位置から読み出しを開始して、各段の現在の表示位置からそれぞれ1個の表示値を読み出し、10種類の、各段の表示値の重み付き和 $b_1 \sim b_{10}$ を採取して、それぞれの重み付き和の、68を法とする剰余 $c_1 \sim c_{10}$ を算出する。この場合の重みは適当に定めればよく、重みの種類ごとに重み付き和が求められる。読み出し機構は、1回の読み出しを行うごとに、各段にお

ける表示位置を1個ずつ右へずらしてゆく。この乱数表の周期は、 $\Pi(89, 83, \dots, 47)$ であり、 $1.8 \times 10^{18}$ 程度である。原写像0～67を表す間接指標配列2は、68個の間接指標配列を並べたものである。各間接指標配列の内容は、適当な乱数を用いて作成することが望ましい。また、間接指標配列の数は、例えば後述のように、原写像の組み合わせの総当たりを試行する攻撃方法の場合と、乱数表の表示開始位置の総当たりを試行する攻撃方法の場合とで、試行回数と実行時間を勘案しながら、適当な値を選択すればよい。

【0034】

【数4】

ける表示位置を1個ずつ右へずらしてゆく。この乱数表の周期は、 $\Pi(89, 83, \dots, 47)$ であり、 $1.8 \times 10^{18}$ 程度である。原写像0～67を表す間接指標配列2は、68個の間接指標配列を並べたものである。各間接指標配列の内容は、適当な乱数を用いて作成することが望ましい。また、間接指標配列の数は、例えば後述のように、原写像の組み合わせの総当たりを試行する攻撃方法の場合と、乱数表の表示開始位置の総当たりを試行する攻撃方法の場合とで、試行回数と実行時間を勘案しながら、適当な値を選択すればよい。

【0039】原写像0～67の逆写像を表す間接指標配列3は、間接指標配列2の各配列に対して、それぞれの逆写像を表す間接指標配列を並べたものである。間接指標配列3を作成するためには、元数89個のソートという操作を、68回行うだけでよい。定数系列の4次行列 $f$ と、 $f$ の逆行列 $g$ は、逆行列が1個存在するように選ばれた、適当な行列である。定数系列の4次行列 $f$ には、単位行列を選んではならないのはもちろんだが、図5(b)に示されたような疎行列も好ましくなく、密行列を選ぶことが望ましい。また、行列の次数は、4次に限らず、例えば4次の倍数で任意に選ぶことができるが、この際、行列の次数と、1回の処理で取り扱う文字列のバイト数とが等しくなるようにすることが必要である。

【0040】次に、図7、図8を用いて、この例の方法によって、平文の暗号化と、暗文の復号化とを行う場合の手順を説明する。まず、発信者に秘密鍵6を指定させることによって、この秘密鍵6から乱数表の各段の開始位置を決定する。秘密鍵6は、その長さを例えば89種類の文字の内から指定する場合には、10バイト以上を入力させることが推奨される。秘密鍵6から10種類の任意の重みを付けた重み付き和 $a_1 \sim a_{10}$ を採取し、それぞれ89を法とする剰余、83を法とする剰余、..., 47を法とする剰余を算出して、乱数表の1段目、2段目、..., 10段目の表示開始位置を決定する(手順S1)。最初、平文データから、4バイトずつの文字列7を順次取り出し(手順S2)、文字列の取り出しごとに、乱数表と読み出し機構1から値を読み出して、使用

する原写像の番号  $c_1 \sim c_5$  と、 $c_6 \sim c_{10}$  を決定する。

【0041】次に、2に示す原写像0を表す間接指標配列～原写像67を表す間接指標配列から、 $c_1$ 番～ $c_5$ 番の配列を取り出し、これらの合成写像を表す間接指標配列  $d_1$  を作成する(手順S3)。同様に、間接指標配列2から、 $c_6$ 番～ $c_{10}$ 番の配列を取り出し、これらの合成写像を表す間接指標配列  $d_2$  を作成する(手順S4)。そして、平文データ中の4バイト文字列を、まず、間接指標配列  $d_1$  で変換し(手順S5)、次に変換結果の文字列を、行列  $f$  との積算で変換し(手順S6)、さらにこの変換結果の文字列を、間接指標配列  $d_2$  で変換して(手順S7)、変換結果の文字列を暗文データ中の4バイト文字列8として格納する(手順S8)。次に、乱数表の各段の表示位置を1個ずつ右へ移動させ、平文データから次の4バイト文字列を読み出して、以下、上記と同様の処理を繰り返す。平文データの、4バイトに満たない終端部分の処理については、例えば、適当なデータをパディングして4バイトの倍数になるような調整を行えばよく、この発明の本質には無関係である。

【0042】受信者が、このようにして生成された暗文の復号化を行う場合にも、上記の秘密鍵6を使用する。暗号化時と同様に、乱数表の各段の表示開始位置を決定する。暗文データから4バイトの文字列を取り出すごとに、暗号化の場合と同様に、原写像の番号  $c_1 \sim c_{10}$  を算出する。次に、3に示す原写像0の逆写像を表す間接指標配列～原写像67の逆写像を表す間接指標配列から、 $c_{10}$ 番～ $c_6$ 番の逆写像の配列を取り出し、これらの合成写像を表す間接指標配列  $e_2$  を作成する(手順S9)。この際、注意すべきことは、暗号化時には、 $c_6, c_7, \dots, c_{10}$  の順に合成したのに対し、復号化時には、逆写像を、 $c_{10}, c_9, \dots, c_6$  の順に合成する点である。

【0043】次に、同様に、間接指標配列3から  $c_5$  番～ $c_1$  番の逆写像の配列を取り出し、これらの合成写像を表す間接指標配列  $e_1$  を作成する(手順S10)。この場合も、暗号化の場合とは逆の順序で合成することに注意する必要がある。なお手順S9と手順S10は、どちらを先に行ってもよい。そして、暗文データ中の4バイト文字列8を、まず間接指標配列  $e_2$  で変換し(手順S11)、次に変換結果の文字列を、逆行列  $g$  との積算で変換し(手順S12)、さらにこの変換結果の文字列を、間接指標配列  $e_1$  で変換して(手順S13)、変換結果の文字列を平文データ中の4バイト文字列として格納する(手順S14)。暗文データの、4バイトに満たない終端部分の処理については、平文データの暗号化の場合と同様に処置すればよい。

【0044】以下、この例の共通鍵暗号化方法による暗文に対して、秘密鍵を知らずに解読を試みた場合の、解

読の可能性について検討する。いま、攻撃者が、暗号化の方法のうち、秘密鍵以外の部分、すなわち乱数表と読み出し機構1と、原写像0～67を表す間接指標配列2と、原写像0～67の逆写像を表す間接指標配列3と、定数係数の4次行列  $f$  と、 $f$  の逆行列  $g$  とを入手していると仮定すると、この場合、攻撃者は、秘密鍵6を知らないで、乱数表と読み出し機構1の上の表示開始位置を、直接には求められない。

【0045】また、攻撃者が、例えば先頭の4バイトに関して、平文と暗文の組み合わせを入手したと仮定すると、この場合、原写像0～67のうち、どれとどれが  $c_1 \sim c_{10}$  として選ばれたかわからないため、間接指標配列  $d_1, d_2$  は、攻撃者にとって未知の写像である。ここで攻撃者が解くべき問題は、「既知の4バイトの文字列が、未知の間接指標配列  $d_1$ 、既知の行列  $f$  との積算、未知の間接指標配列  $d_2$  を経て、既知の4バイトの文字列となった場合の、間接指標配列  $d_1, d_2$  を求めよ。また、乱数表上の表示位置を求めよ。」ということになるが、この問題を解析的な手法で解くことはできない。

【0046】また、攻撃者が、既知の平文と暗文の組み合わせ、又は、選択した平文と暗文の組み合わせから、差分をとって解析することを考えたと仮定すると、この発明の暗文は、間接指標配列による変換という、線形的な性質とは無縁の写像であって、行列の積算による変換を挟んだ形になっているので、差分解析は不可能である。

【0047】また、攻撃者が、例えば先頭の4バイトに関して、平文と暗文の組み合わせを多数入手して、対応表を作ることで問題を解くことに代えようとしたと仮定すると、この場合は、単純に計算すれば、 $89^4$  すなわち6千2百万個以上程度の組み合わせを入手しなければならない。既知平文攻撃とは、なんらかの事情で、平文が既知であるもののうち、相手側が同じ秘密鍵を用いて暗号化した暗文を入手できた場合に成立するものであるが、相手側が、6千2百万回も同じ秘密鍵を用いることを期待しても、それは、事実上不可能である。

【0048】また、攻撃者が、以下のような選択平文攻撃を試みた場合を仮定する。すなわち、全文が一定の4バイトの文字列の繰り返しであるような平文データ、例えば、「comp」、「entr」、「conc」、「symm」、「able」、「then」、「than」、「here」等のような4バイトの文字列の繰り返しの平文データを作成する。そして、平文中に出現する頻度が高いと思われる文字列をつぎつぎに試行し、相手側に同じ秘密鍵で暗号化させて、暗文を入手する。また、同様に、上記の文字列が4バイトの整数倍の区切りに対して、1バイト、2バイト、又は3バイト目に出現した場合に相当する平文データを作成し、相手側に同じ秘密鍵で暗号化させて、暗文を入手する。

【0049】つまり、出現する頻度が高いと思われる文字列1個につき、4通りの平文データを選択する。そして、対応表を作って目的の暗文と比較すれば、目的の暗文中の一定の位置に一定の文字列が出現した場合、当該位置の平文が判明する。ただし、この手法での攻撃を意味のあるものにするためには、どんなに少なくとも、50種類の文字列×4回程度以上の試行が必須と考えられる。選択平文攻撃とは、攻撃者が選択した平文を、なんらかの詐術を用いて、相手側に秘密鍵で暗号化させて、その暗文を入手することによって成立する。しかしながら、200回以上もの選択平文攻撃を仕掛けられるなどということは、現実には考えられないことである。もしも、それが可能なほどの事情があるならば、秘密鍵を教えてもらうことのほうが、よほど簡単であろう。

【0050】また、攻撃者が、乱数表と読み出し機構1を用い、表示開始位置の総当たりを試行したと仮定する。既述の通り、乱数表の周期は、 $1.8 \times 10^{18}$ 程度である。そこで、1秒間に1億回の試行を行うことが可能な計算機又は専用のハードウェアがあったとしても、この試行には、570年以上かかることになる。

【0051】また、攻撃者が、秘密鍵の総当たりを試行したと仮定する。発信者が秘密鍵の長さとして10バイトの文字列を用いていて、「10バイト」という長さだけが既知であったとすると、可能な組み合わせは、 $31 \times 10^{18}$ 程度である。そこで、1秒間に1億回の試行を行うことが可能な計算機又は専用のハードウェアがあったとしても、この試行には、9800年以上かかることになる。

【0052】また、攻撃者が、間接指標配列d1、d2の総当たりを試行したと仮定すると、89の階乗は、 $16 \times 10^{135}$ 程度であるから、間接指標配列そのものの可能性をいちいち試すなどということは、絶対不可能なことである。そこで、原写像0～67のうち、10個のものが選ばれて合成されることから、可能な順列を総当たりで試行することになるが、可能な順列は $68^{10}$ であって、 $2 \times 10^{18}$ 程度になり、上記の場合と同じ条件として、600年以上かかることになる。

【0053】この例の方法は、古典的な暗号化方式と比較すれば、「無限に近い長さの周期を持つ多表式暗号と、綴字換字暗号とを組み合わせたもの」に相当する。将来、計算機又は専用ハードウェアで実現できる実行速度が著しく改善され、上記各例で説明したような総当たりが可能になった場合には、乱数表の段数及び各段の幅と、合成写像に用いる間接指標配列の個数を定量的に増やすだけで対応でき、暗号化方式自体の定性的改変は必要とされない。

【0054】このように、この例の共通鍵暗号化又は復号化方法によれば、長周期の乱数表と、乱数によって間接指標配列の順列を変化させる機構と、間接指標配列による変換で定数係数行列との積算を挟む形の合成写像と

を有しているので、既知平文攻撃並びに選択平文攻撃を事実上不可能にすることができる。

#### 【0055】◇第2実施例

図9は、この発明の第2実施例である共通鍵暗号化又は復号化方法において、使用開始前に決定し配布される事項を説明する図、図10、図11は、同実施例の方法における暗号化と復号化の手順を説明する図である。この例においては、図9に示す、乱数表と読み出し機構11と、原写像0～67を表す間接指標配列12と、原写像0～67の逆写像を表す間接指標配列13と、定数係数の4次行列f14と、fの逆行列g15とは、共通鍵暗号化又は復号化方法の使用開始前に、別途決定され、配布されているものとする。

【0056】ここで、乱数表と読み出し機構11、原写像0～67を表す間接指標配列12、原写像0～67の逆写像を表す間接指標配列13、定数係数の4次行列f14、fの逆行列g15は、それぞれ、図6に示された、乱数表と読み出し機構1、原写像0～67を表す間接指標配列2、原写像0～67の逆写像を表す間接指標配列3、定数係数の4次行列f4、fの逆行列g5と同様なので、以下、これらについての詳細な説明は省略する。

【0057】次に、図10、図11を用いて、この例の方法によって、平文の暗号化と、暗文の復号化とを行う際の手順を説明する。まず、発信者に秘密鍵16を指定させることによって、この秘密鍵16から乱数表の各段の開始位置を決定する手順は、図7、図8に示された第1実施例の場合と同様である（手順P1）。最初、平文データから、4バイト×256要素のベクトル17を取り出し（手順P2）、乱数表と読み出し機構11から256回分の読み出しと、使用する原写像の番号c1～c10の算出を行い、要素ごとに使用する原写像番号c1～c5を格納した作業ベクトル18に格納し（手順P3）、要素ごとに使用する原写像番号c6～c10を格納した作業ベクトル19に格納する（手順P4）。なお、平文データから取り出すバイト数は、4バイトに限らないことは第1実施例の場合と同様であり、これと行列の次数との関係も同様である。また、要素数も256要素に限らず、例えば、512要素でもよい。

【0058】次に、平文データ中の4バイト×256要素のベクトル17の各要素を、要素ごとに使用する原写像番号c1～c5を格納した作業ベクトル18の各要素に含まれる、c1～c5が指し示すところの原写像を用いて変換する（手順P5）。この操作はリストベクトルロードと呼ばれ、ベクトルパイプライン演算器を持つ計算機では、高速に実行できる。次に、上記の操作で得られたベクトルの各要素を、行列fとの積算で変換する（手順P6）。この操作は線形演算であり、ベクトルパイプライン演算器を持つ計算機では、高速に実行できる。次に、上記の操作で得られたベクトルの各要素を、

要素ごとに使用するc6～c10を格納した作業ベクトル19の各要素に含まれる、原写像番号c6～c10が指し示すところの原写像を用いて変換する(手順P7)。この操作は、上記と同様にリストベクトルロードであり、ベクトルパイプライン演算器を持つ計算機では、高速に実行できる。そして、変換結果のベクトルの各要素を、暗文データ中の4バイト×256要素のベクトルとして、暗文データ中に格納する(手順P8)。

【0059】このようにして作成された暗文を復号化するには、第1実施例の場合と同様に、逆写像、逆行列を用いて同様の手順によって行うことができる。暗号化時と同様に、乱数表の各段の表示開始位置を決定する。暗文データから4バイト×256要素のベクトル20を取り出すごとに、乱数表と読み出し機構11から256回分の読み出しと、使用する原写像の番号c1～c10の算出を行って、要素ごとに使用する原写像番号c10～c6を格納した作業ベクトル21に格納し(手順P9)、要素ごとに使用する原写像番号c5～c1を格納した作業ベクトル22に格納する(手順P10)。なお、手順P9と手順P10は、どちらを先に行ってもよい。

【0060】次に、暗文データ中の4バイト×256要素のベクトル20の各要素を、要素ごとに使用する原写像番号c10～c6を格納した作業ベクトル21の各要素に含まれる、c10～c6が指し示すところの原写像の逆写像を用いて変換(リストベクトルロード)し(手順P11)、変換結果の4バイト×256要素のベクトルの各要素を、行列fの逆行列gとの積算で変換(線形演算)し(手順P12)、変換結果の4バイト×256要素のベクトルの各要素を、要素ごとに使用する原写像番号c5～c1を格納した作業ベクトル22の各要素に含まれる、c5～c1が指し示すところの原写像の逆写像を用いて変換(リストベクトルロード)して(手順P13)、変換結果の4バイト×256要素のベクトルを平文データ中の4バイト×256要素のベクトルとして、平文データに格納する(手順P14)。暗文データの、4バイトに満たない終端部分の処理については、平文データの暗号化の場合と同様に処置すればよい。

【0061】このように、この例の共通鍵暗号化方法によれば、長周期の乱数表と、乱数によって間接指標配列の順列を変化させる機構と、間接指標配列による変換で定数係数行列との積算を挟む形の合成写像とを有しているので、既知平文攻撃並びに選択平文攻撃を事実上不可能にすることができる。

【0062】この例の共通鍵暗号化方法による暗文に対しても、既知平文攻撃並びに選択平文攻撃が事実上不可能である。その理由は、第1実施例について説明したのと同様なので、詳細な説明は省略する。

【0063】以上、この発明の実施例を図面により詳述してきたが、具体的な構成はこの実施例に限られたもの

ではなく、この発明の要旨を逸脱しない範囲の設計の変更等があってもこの発明に含まれる。例えば、この発明をソフトウェアによって実現する場合は、ハードウェアとして、汎用機、ワークステーション、パーソナルコンピュータ等、適当なコンピュータシステムを備え、これにこの発明の方法を実行するためのプログラムを装備することによって容易に実現できる。さらに、このようなプログラムを、処理装置が読み取り可能な、任意の形式の媒体に記録した状態で予め用意することによって、同様なシステムを具備する場合に、同一の方法を普遍的に実現することができる。

#### 【0064】

【発明の効果】以上説明したように、この発明によれば、長周期の乱数表と、乱数により間接指標配列の順序を変化させる機構と、間接指標配列による変換で定数係数との積算を挟む形の合成写像とを有しているので、既知平文攻撃並びに選択平文攻撃を事実上不可能とする、共通鍵暗号化又は復号化方法を実現するとともに、共通鍵暗号化又は復号化プログラムを記録した記憶媒体を提供することができる。

#### 【図面の簡単な説明】

【図1】写像において、文字と数値を対応させる場合の例を示す図である。

【図2】この発明の一実施の形態における間接指標配列による写像の仕組みについて示す図である。

【図3】同実施の形態における間接指標配列による写像の逆写像について示すための図である。

【図4】同実施の形態における行列の積算による写像の仕組みについて示すための図である。

【図5】同実施の形態における逆行列の積算による逆写像の仕組みについて示すための図である。

【図6】この発明の第1実施例である共通鍵暗号化又は復号化方法において、使用開始以前に決定し配布される事項を説明する図である。

【図7】同実施例の方法における暗号化と復号化の手順を説明する図である。

【図8】同実施例の方法における暗号化と復号化の手順を説明する図である。

【図9】この発明の第2実施例である共通鍵暗号化又は復号化方法において、使用開始前に決定し配布される事項を説明する図である。

【図10】同実施例の方法における暗号化と復号化の手順を説明する図である。

【図11】同実施例の方法における暗号化と復号化の手順を説明する図である。

#### 【符号の説明】

- |       |                      |
|-------|----------------------|
| 1, 11 | 乱数表と読み出し機構           |
| 2, 12 | 原写像0～67を表す間接指標配列     |
| 3, 13 | 原写像0～67の逆写像を表す間接指標配列 |

- 4, 14 定数係数の4次行列  
 5, 15 定数係数の4次行列の逆行列  
 6, 16 秘密鍵  
 7 平文データ中の4バイト文字列  
 8 暗文データ中の4バイト文字列

- 17 平文データ中の4バイト×256要素のベクトル  
 トル  
 20 暗文データ中の4バイト×256要素のベクトル  
 トル

【図1】

1

対象文字が89種の場合の文字—数値間の対応の例

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
&	;	(	)	*	+	.	-	/	0	1	2	3	4	5	
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
6	7	8	9	:	:	<	=	>	?	@	A	B	C	D	E
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
V	W	X	Y	Z	[	¥	]	^	_	a	b	c	d	e	
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
80	81	82	83	84	85	86	87	88							
v	w	x	y	z	{		}	~							

【図3】

- (a) 逆写像を表す間接指標配列の説明  
 指標配列 $x(i=0\sim 88)$ を  
 間接指標配列 $c(j=0\sim 88)$   
 で変換して  
 配列 $(0,1,\dots,88)$ になる場合。  
 配列 $x(i=0\sim 88)$ を間接指標配列と  
 見做して表される写像は  
 配列 $c(j)$ の表す写像の逆写像である

- (b) 逆写像を表す間接指標配列の例  
 指標配列 $(87,88,0,1,\dots,48,\dots,58,\dots,85,86)$ を  
 2番 50番 60番 87番 88番  
 間接指標配列 $(2,3,\dots,52,\dots,62,\dots,88,0,1)$   
 0番 50番 60番 86番 88番  
 で変換すると  
 配列 $(0,1,2,\dots,87,88)$ になる

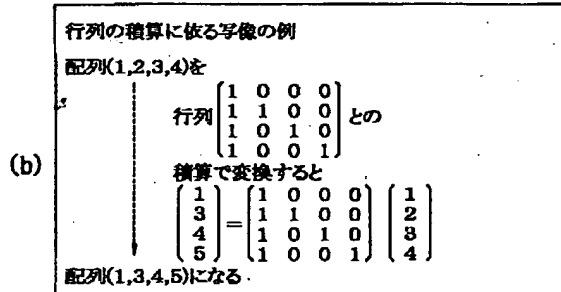
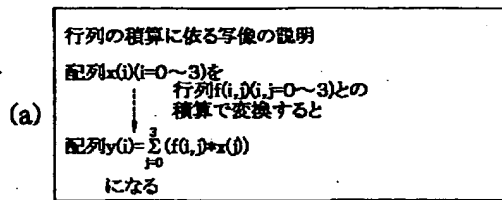
【図2】

- (a) 指標と間接指標配列に依る写像の説明  
 指標 $x$ を  
 間接指標配列 $c(j=0\sim 88)$ で  
 変換すると  
 $y=c(x)$ になる  
 指標配列 $x(i=0\sim 9)$ を  
 間接指標配列 $c(j=0\sim 88)$ で  
 変換すると  
 配列 $y(i=c(x(i)))$ になる
- (b) 写像の例  
 指標配列 $(50,60,70,80)$ を  
 間接指標配列 $(2,3,\dots,52,\dots,62,\dots,88,0,1)$   
 0番 50番 60番 86番 88番  
 で変換すると  
 配列 $(62,62,72,82)$ になる
- (c) 合成写像の例  
 指標配列 $(50,60,70,80)$ を  
 間接指標配列 $(2,3,\dots,52,\dots,62,\dots,88,0,1)$   
 0番 50番 60番 86番 88番  
 で変換し、更に  
 間接指標配列 $(1,2,3,\dots,53,\dots,63,\dots,83,\dots,88,0)$   
 0番 52番 62番 82番 88番  
 で変換すると  
 配列 $(53,63,73,83)$ になる

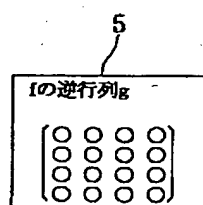
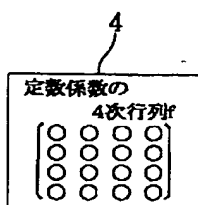
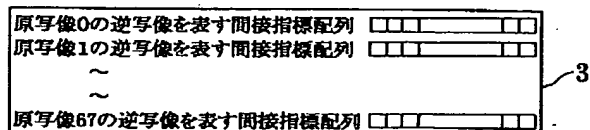
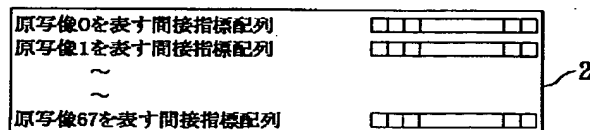
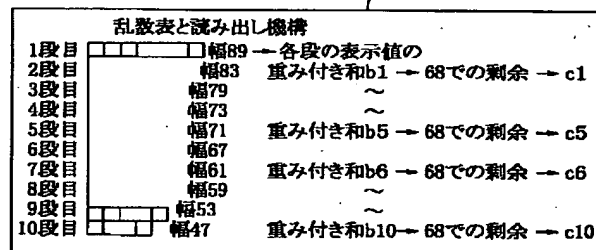
【図7】

- 6  
 秘密鍵  
 (S1)  
 重み付き和 $a_1 \rightarrow 89$ での剰余  $\rightarrow$  乱数表1段目の開始位置  
 重み付き和 $a_2 \rightarrow 83$ での剰余  $\rightarrow$  乱数表2段目の開始位置  
 重み付き和 $a_9 \rightarrow 53$ での剰余  $\rightarrow$  乱数表9段目の開始位置  
 重み付き和 $a_{10} \rightarrow 47$ での剰余  $\rightarrow$  乱数表10段目の開始位置

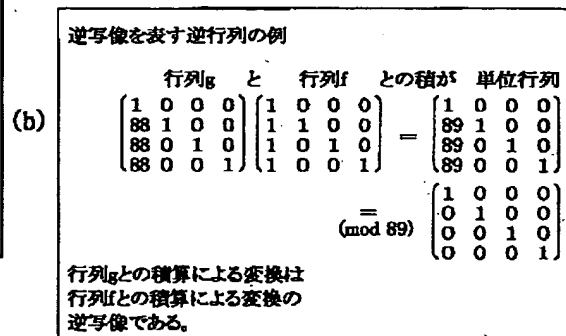
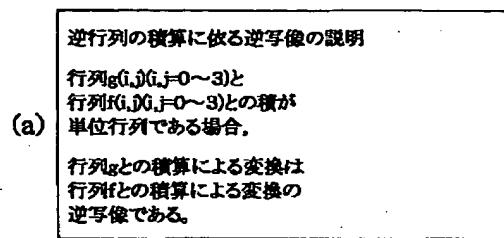
【図4】



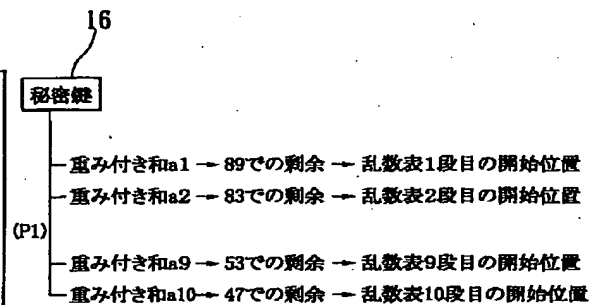
【図6】



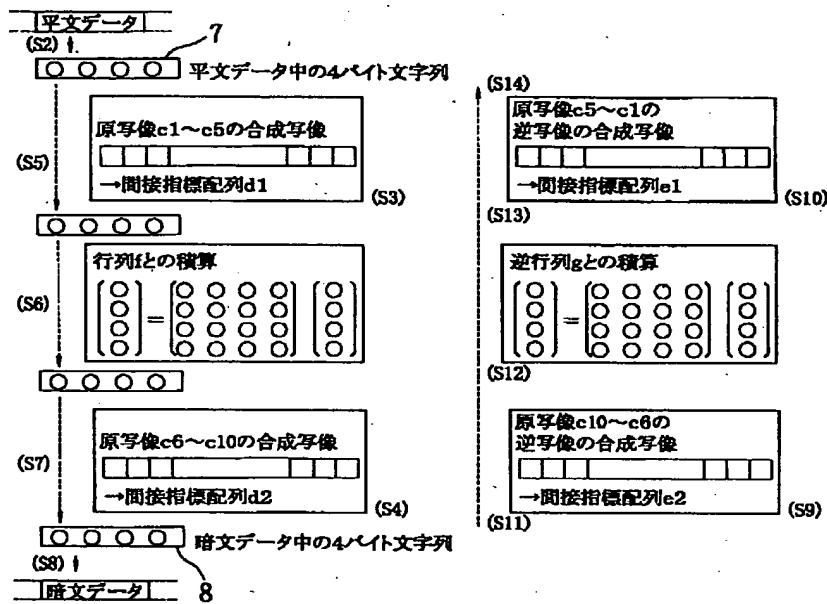
【図5】



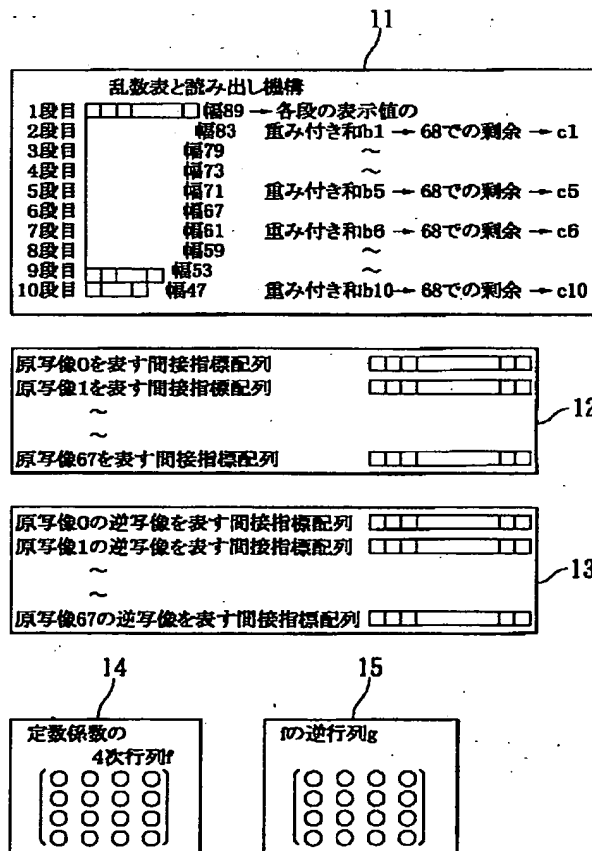
【図10】



【図8】



【図9】





【図11】

